STATE OF ALABAMA
INFORMATION SERVICES DIVISION

Personally Identifiable Information (PII)

Information Technology Policy 680-01: Information Protection

Information Technology Standard 680-01S2
Protecting Personally Identifiable Information

Definitions

- Personally Identifiable Information (PII)
  - Any information about an individual such as their name, Social Security number, date and place of birth, mother's maiden name, biometric records, etc.
- Individual
  - A living person who is a citizen of the United States or an alien lawfully admitted for permanent residence.
- Individual Identifier
  - Information associated with a single individual such as name, Social Security number or other identifying information.

Definitions (cont'd)

- Identifying Information
  - Name
  - Date of Birth
  - Social Security Number
  - Financial Information
  - Biometric Data
  - Fingerprints
  - Passwords
  - Parent's surnames

Definitions (cont'd)

- PII Electronic Record
  - Any item, collection, or grouping of information in electronic form that associates personal information with an individual identifier.
  - Electronic records that contain information about education, financial transactions, medical history, or criminal or employment history but do not include individual identifiers are not considered PII electronic records.

Introduction

- State IT Standard 680-01S2
  - Protecting Personally Identifiable Information (PII), establishes requirements for the protection of electronic records containing PII that is either accessed remotely or physically transported or stored on mobile devices.
- Objective
  - Protect PII electronic records from unauthorized modification, disclosure, or loss.
- Scope
  - These requirements apply to all State-owned or controlled information systems or services that receive, process, store, display or transmit State information regardless of classification or sensitivity (includes contracted or outsourced access to State information and resources).

Requirements

- Confirm PII Protection Needs
  - Ensure information system owners and data owners identify PII and evaluate risk.
  - All PII not explicitly cleared for public release shall be protected.
  - All PII shall be evaluated for impact of loss or unauthorized modification or disclosure and protected accordingly.

Requirements (cont'd)

- PII Transported/Stored Off-Site
  - Electronic PII records shall not be routinely processed or stored on mobile computing devices or removable electronic media.
  - Except for compelling operational needs, any mobile computing device or removable electronic media that processes or stores electronic PII records shall be restricted to secured workplaces.
  - Any mobile computing device containing electronic PII records removed from the workplaces, must be signed in and out with an authorized official designated in writing by the organization's senior agency management.

Requirements (cont'd)

- PII Remote Access Protections
  - Remote access to PII records is permitted only for compelling operational needs, and:
    - Shall employ certificate based authentication.
    - Any remote device gaining access shall implement a screen lock control with a specified period of inactivity not to exceed 15 minutes.
    - Download and storage of PII records is prohibited except as described in this standard and only if expressly approved by the data owner.
  - Only State authorized devices shall be used for remote access. All remote access shall comply with applicable State standards.

Requirements (cont'd)

- Data Loss Procedures
  - The Information Security Officer (ISO) of the Information Services Division (ISD) of the Department of Finance shall establish procedures for reporting the compromise, loss, or suspected loss of PII per 600-04P1.
  - Heads of State Entities shall:
    - Establish reporting procedures to ensure that compromise, loss, or suspected loss of PII is reported in accordance with State requirements.
    - Ensure supervising officials establish logging and tracking procedures for electronic PII records on mobile computing devices or portable media removed from protected workplaces.

Things You Should Do to Protect PII

- Familiarize yourself with PII policy
- Remove PII from non-secure areas (e.g., desktops, folders, community cabinets)
- Secure PII in locked containers (cabinets, drawers)
- Report suspected or known PII vulnerabilities
- Encrypt PII data stored off-site (e.g., tapes, storage devices, flash drives)
- Ensure secure access to areas displaying PII
- Perform risk assessments

Things You Should NOT Do With PII

- Do not store personal PII on State equipment
- Do not reveal PII to unauthorized individuals
- Do not discard PII into non-secure waste containers
- Do not transport/store PII on unauthorized storage devices
- Do not remove/transport PII without data owner's written permission
- Do not email unprotected PII

Recent Incidents of PII Disclosures

- **Data Breach Affects Thousands of Ohioans (June 2007)**
  - Stolen backup storage device
  - All 64,000 state employees names, SSNs, dependents info
- **California State Pension Fund Admits Breach (Aug 2007)**
  - 445,000 state employees PII inadvertently printed by Agency
  - SSNs printed on brochures announcing upcoming election
- **IBM Tapes Lost After Traffic Accident (May 2007)**
  - Consumer tapes with PII of current & former employees
  - Tapes in a contractor vehicle involved in an accident
- **Veterans' Data Swiped in Theft (May, June & August 2006)**
  - 26.5 million U.S. veterans PII info stolen from govt. employee home by teenagers
  - 6,744 records pertaining to "mustard gas veterans" testing during WWII was breached
  - Unisys (subcontractor) can't find 38,000 vet's data – PII missing when desktop was stolen

Additional Information

- **Policy**
  - Information Technology Policy 680-01: Information Protection
- **Related Documents**
  - Information Technology Standard 680-01S1: Information Protection
  - Information Technology Standard 650-01S1: Physical Security
  - Information Technology Procedure 600-04P1: Cyber Security Incident Reporting
- **Web Site for Policy and Related Documents**
  - http://isd.alabama.gov/policies/policies.aspx